The Court Has Been Hacked!

By Judge Herbert B. Dixon Jr. (Ret.)

The most horrible day of Judge Hank's tenure as chief judge began with the ringing of his bedside phone. It took a moment for the sound to register as he was roused from sleep. He saw the time and wondered who would be calling at 4:00 a.m., and why? As he reached for the phone, caller ID identified the court's newly hired IT director, a nationally recognized tech wizard, ironically named Circuit Board.

"Hello."

"Good morning, Chief."

"Well, Circuit, I'd say it's barely morning. 4 a.m."

"Yes, I'm sorry to wake you at this hour, but we have an emergency on our hands. The court has been hacked."

"Hacked?"

"Our entire system has been compromised. A pop-up note appears on the court's start-up screen saying the 'Enemy of Justice' has taken over the court's system. It or they have not—there has not been any demand. The note said that they wanted us to savor the experience, then they'll get back to us."

"What does that mean?" asked Chief Judge Hank.

"Well, I think we'll only fully realize that over the coming hours or days, but I can tell you that emails can't be accessed, nor the daily court calendars of cases. Also, judicial dockets are offline, so we have no access to schedules, pleadings, orders, or other documents."

"Good Heavens."

"Additionally, Chief, the court's telephone service is down. Several years ago, the court switched from analog landline service to digital VOIP—Voice Over Internet Protocol. This VOIP phone system is part of the court's network that has been compromised. We maintained a few analog lines in case of an emergency."

"Like this one?" interrupted the chief.

"Yes, sir," replied Circuit, "and we can install and activate additional analog lines in some offices to help us through this situation."

After receiving additional information from IT Director Circuit Board, Chief Judge Hank called his assistant to schedule an 8:00 a.m. meeting with the clerk of the court and the court's division directors and presiding judges. The chief got out of bed and started getting ready. There was no more sleep to be had today.

Chief Judge Hank parked at his court parking space and headed to the court personnel entrance. He swiped his key card several times, but the door wouldn't open. He remembered he had a master key, which he rarely used. He found it on his chain, tried it, and luckily it worked. The chief went in and decided to take the long way to his office to see what was occurring in the public areas of the court.

Despite the early hour, some of the typical hallway activities had begun. Opposing counsel were conducting meet and confer gatherings, lawyers were meeting clients and witnesses, and family members were searching for each other. Lines were beginning to form at the courthouse entrances, where the guards were experiencing connectivity problems with their main office. Little did everyone realize what this day had in store for them.

The chief judge arrived for the emergency meeting and was greeted with a

nearly empty conference room, save for Circuit Board, the IT director.

"So, where is everyone?" asked the chief.

"I've received calls on my cell from a few of the division directors. Their key cards are not functioning. They had to go to the public entrances."

"Circuit, why has this happened? You reported in your initial study of our IT infrastructure that the key card system needed to be separated from the network to minimize multiple system failures," said the chief judge. "That's true, Chief. The contract bid solicitation for that work is pending with procurement. We were expecting the work to be done next month."

"Oh, brother."

Over the next few minutes, the clerk of the court, division directors, and presiding judges started arriving, several of them soaking wet. Etchings of tension and confusion on their faces were obvious.

"Deborah, are you okay?" Chief Judge Hank asked the clerk of the court.

"Chief, our key cards would not work at the employee entrance, and it started raining while we walked to a public entrance and waited to go through security," said Deborah as she pushed her soaked hair away from her face.

Once everyone was settled, the chief judge turned to the IT director. "What actions have we taken so far to deal with this?"

"We've begun going through, identifying, and isolating all infected system applications."

"Circuit, wouldn't it be better to shut down the whole system?"

"Not really, Chief. Within the system's transient memory, there may be clues regarding what exactly happened. For instance, the problem may have started with an employee inserting an infected flash drive into his office computer, or visiting a dangerous website, or clicking on a malicious link in an email. There are numerous ways this hack could have happened. If we shut down everything, we lose that transient memory and much of our ability to investigate the hack's origins. And shutting down the whole system will slow down our efforts to determine how extensively we have been compromised."

"And what can be done about those parts you determine are infected?"

"Well, we will determine if we can recover the data and rebuild the database. But this brings up a discussion when I was hired about the absence of a daily backup system, regular testing of the backups, and the implementation of continuous cloud backup." All eyes in the room focused on IT Director Circuit Board as he continued. "With cloud services, we would be able to access applications, programs, and data as soon as we restored internet access and not be dependent on what's stored on the court's network and individual hard drives. Unfortunately, because of fiscal restraints, we put those efforts in next year's budget."

Audible groans in unison cascaded across the otherwise silent room, including a few barely audible expletives.

A pit began forming in the chief judge's stomach. He turned to the clerk of the court. "Deborah, what can you tell us?"

"We're still assessing our situation, Chief. We know we can't access the judicial dockets or court calendars. We're also unable to vacate or schedule hearings electronically, which is quite a problem because we need to do a lot of rescheduling because of Circuit Board's techno-fiasco."

"Chief!" responded Circuit.

"Now, now, everyone," said Chief Judge Hank. "Let's stick to identifying the problems and finding solutions."

Deborah continued, "We have to resort to paper, which will slow things down dramatically. We are reaching out to division directors, courtroom clerks, and individual judges to see what information they have. They typically print advance copies of their daily calendars for personal use and to post on courtroom doors. But our telephone system is down. We have no email, internet service, telephone service, electronic case management system—nothing, zip, nada, zilch, nil, goose egg, naught, zero—."

"Stop, Deborah," said the chief judge, "this is not helpful."

"Okay, Chief. I am just so angry and frustrated," said Deborah. "We are a digital operation! Any paper copy of a past or current record is completely fortuitous and most likely was printed for someone's convenience. We stopped maintaining paper files over 15 years ago. We are doing our best to build a hard copy of the master calendar. Welcome back to the 1980s."

Jackson, the Civil Division director, spoke up. "Chief, we use a third-party vendor for our electronic filing, and I called them when I heard about our problem. Our liaison told me that their system has not been affected by this outage. They are still receiving pleadings and other filings. The problem now is they cannot transmit the filings to the court, but all filings during this outage will be securely maintained and available to the court when our problem is solved."

"Okay. That's some good news, I think," said the chief judge, with both hands over his face. "Who else has information?"

Judge King, presiding judge of the Civil Division, spoke up. "We currently can't access any trial or hearing records. Both trial recordings and transcripts are stored electronically. It will, of course, be difficult for judges to render a decision in a case when they don't have access to the prior court record. We are also looking at a loss, perhaps a permanent loss, of massive amounts of work product, final and draft versions of orders, decisions, and research memoranda. Any work stored solely on the court's network could be lost forever if it has not been transmitted to an outside account. Judges and their law clerks could

Judge Herbert B. Dixon Jr. retired from the Superior Court of the District of Columbia after 30 years of service. He is a former chair of both the National Conference of State Trial Judges and the ABA Standing Committee on the American Judicial System and a former member of the Techshow Planning Board. You can reach him at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.

be starting over from scratch. And trying to re-create files of orders by attempting to claw back versions we sent out to parties will be tedious, to say the least, with a likely incomplete result."

The chief judge turned to the director of the Criminal Division. "Is there anything you want to add, Reggie?"

"Similar to what the other divisions are experiencing, Chief; because the motions tracking system is linked to the court's electronic docket, we are not receiving any notifications of time-sensitive motions that need to be addressed or other events that are requiring immediate action. We can't issue or quash criminal warrants. Because the court's email is down, we're also not receiving notifications, such as probation and parole violations. There are plenty of other things that will be tied up on our end, such as the ability to effectuate prisoner transfers so that they can attend hearings, return property seized as evidence, and compensate the appointed defense counsel. We don't have access to the criminal justice fund for payment of those fees."

Herman, the Human Resources director, spoke up. "We need to know if Social Security numbers and other personal identifiable information have been compromised. Even worse, if we don't find a way to process payroll this week, we will have an employee revolt on our hands."

The room went silent for almost a full minute.

The director of the Landlord and Tenant Division announced that the court was now unable to accept tenants' payments of funds into the court's escrow account to avoid a premature eviction while awaiting trial. The director of the Traffic Court lamented being unable to collect parking and traffic fines and clear citations. Somebody else also reported that the court's website was frozen, and the electronic monitors posted around the courthouse were dark, which would have an adverse effect on thousands of litigants, attorneys, witnesses, interested parties, and family members who relied on those resources to check the status of scheduled cases.

After hearing too many descriptions of inoperable systems around the courthouse, Chief Judge Hank recessed the meeting so that everyone could continue their best efforts to find and implement any available solutions—everyone, that is, except Circuit Board, with whom the chief judge needed to discuss a court-wide recovery plan. The chief judge walked back to his office with the IT director through an air of confusion that permeated the courthouse halls. Courtroom clerks and other staff were speaking with groups of people trying to determine who they were and which case they were there for, asking for a telephone number or email address they might contact when the court's systems became operational again, repeating multiple times they did not know when the court systems would again be functional, and promising the parties and attorneys they would be contacted by telephone or email before any action was taken in their case.

When they reached the chief judge's chambers, the city attorney was waiting at the door.

"Well, hello, Annette, to what do I owe this visit?"

"I'm sure you've got your hands full right now, your honor, but I tried calling several times, and there's no way to get through to the court."

"Yes, I know, Annette," said the chief. "The court has been hacked. We're still trying to determine the extent to which our digital infrastructure has been compromised. Unfortunately, we know our electronic case management system, telephone, internet service, and much more have been brought to a standstill. Now, Annette, what bad news have you come to share?"

"Our office is very concerned that the hackers have access to highly sensitive information from our case filings that are stored on the court's docket—particularly sealed cases with confidential information implicating trade secrets, witness safety, and maybe even national security concerns. Have you been able to assess whether any of that information has been compromised?"

The chief judge looked at Circuit, who responded, "We're unable to tell at this point, but I'd have to say it's all potentially vulnerable," wishing he could sink through the floor at that moment.

The chief judge and IT director exchanged personal cell phone numbers with the city attorney before she left the court.

"We should expect to receive a lot more inquiries like that about the attack," said Circuit.

"From whom?"

"Well, from attorneys—the public defender's office, the law firms, and advocacy groups from all across the city. Also, the mayor, the governor, the city council, the school board, the Public Utilities Commission, the attorney general, the state legislature—you name it. They will have similar confidentiality concerns and will be wondering what kind of delay this will cause for their cases."

"Unfortunately, Circuit, you are correct," said the chief judge. "Based on all I've heard this morning, the attack may have brought the city's entire legal system to a standstill. If we start creating a list, we'll find a host of other individuals, businesses, and government agencies that rely on court records. All of that is now on hold. They will certainly be concerned. So, Circuit, what's next?"

"We are already doing everything we can to fully assess the damages, isolate affected applications, and await further contact from the hackers. And while we are doing all of that, we will go into recovery mode to the extent we can. Meanwhile, we will update law enforcement each step of the way."

"This is a nightmare—an embarrassing, terrifying nightmare!" said the chief judge.

Meanwhile, thousands of miles away, in a foreign country hostile to the interests of the United States, images from one of the court's confidential internal documents lit up a hacker's screen.

"See, I told you someone from the court would click the link in my email and unleash my new ransomware program. I win the bet!"

"Fine, fine," agreed the other hacker. "Drinks are on me tonight. So, should we reach out to them yet with our demands?"

"There is no rush. Let's monitor Twitter and watch the U.S. news reports about their disaster—at least make them sweat for a few more hours. Besides, we have several other hacking candidates in the queue."

Epilogue

Over the years, I have written several articles for this column that addressed issues of hacking, cybersecurity, and IT disaster prevention and recovery. Here, I wanted to provide a possible worst-case scenario involving a courthouse hacking to get readers' attention. This article is intended as a wake-up call to our readers who have not thought seriously about threats to a court's IT infrastructure. This narrative was intended to give readers a sense of what a worst-case scenario might look like from the inside and to visualize a ransomware attack on your court.

While this is a fictional account and the names of all personnel are imaginary, versions of this nightmare have been experienced by court personnel throughout the country. Recent news accounts have detailed ransomware and other hacking attacks on city and state government institutions, federal agencies and courts, banks, hospitals, the meatpacking industry, and numerous commercial institutions. Given the key role that our courts play to a functioning society, and the enormous quantities of data they hold, including highly sensitive and personal information, the threats of cyber assault will continue. Comparing court institutions with the massive 2017 Equifax hack, Joseph Baxter, the 2020–2021 president of the Conference of State Court Administrators, stated that "the judiciary has all that information and then some and in greater volumes that dwarf those private companies."[1] Further, the vulnerability of courts continues to increase as they implement the use of smartphones and other connected devices for increased productivity, as the breach of one of these devices often serves as the entry point for the takeover of the main system.[2]

This is our current reality, and courts must continue with proactive innovation to prevent future attacks, detect those attacks, and respond to those attacks that succeed. The most respected IT professionals recognize that the probabilities don't rest with "if we are hacked" but "when we are hacked." Accepting that premise of eventuality, it is understandable why the generally accepted four-prong approach for IT defense is prevention, detection, isolation, and recovery. All court employees must do their part with step 1, prevention, to minimize the number of occasions when you hear the refrain, "The court has been hacked!" ■

Judge Dixon wishes to thank James L. Anderson, Esq., Superior Court of DC, senior judges' law clerk, for research and writing assistance preparing this article.

Endnotes

1. Tim Starks, *The Cyberthreat to U.S. Courts*, Politico (July 13, 2020), https://politi.co/3fF486e.

2. *US Criminal Court Hit by "Conti" Ransomware*, Sec. Mag. (Sept. 14, 2020), https://bit.ly/3fEx7XK.